

## **Broadening definitions of personal data portend greater scope of concern for privacy offices**

By Jay Cline, CIPP  
Inside 1to1: Privacy  
June 2011

The privacy footprint is growing. From Sacramento to London and from Bonn to New Delhi, the definitions of personal data and sensitive personal data are expanding. For privacy offices and marketing departments, this means their 2011 agendas just got more crowded--and more intermingled.

What is "personal data"? Many organizations have been answering this question in their data-classification policies with a definition similar to this: Personal data is information that is associated with an individual's name. For these organizations, differentiating between personal data and non-personal data is important. Once data falls into the "personal data" category, use and disclosure restrictions often apply, rendering that data less usable. In the Information Age, data utility can make or break a business model.

"Data classification changes make yesterday's standard operating procedure a disallowed practice today," said Hayden Creque, head of [Creque Law](#) and formerly general counsel of software company W3i.

### **From anonymous to personal data**

So it was no small development in March when the Supreme Court of California ruled in the case of [Pineda vs Williams-Sonoma](#) that zip codes were personal data. How did they reach that landmark conclusion? By determining that postal codes--when collected at the point of sale--could be used along with the payment information to obtain consumer addresses.

What's the impact of this development? California-based retail stores may no longer be able to easily ask for zip codes at the register in order to plan where to build new stores, for example. And gas stations may not be able to ask for zip codes at the pump to deter and detect fraud. Because of the economic importance of the California market, this ruling could also set a precedent for others.

Something more groundbreaking has been unfolding in Europe.

Some EU member states have been defining IP addresses as personal data. Why? Because these addresses--which are numbers assigned to devices on a network in a geographical area--could be linked to individuals if other information is known about them, such as their Internet search patterns. In February, the data protection commissioner from the German state of Lower Saxony [stated](#) that IP addresses can't be shared with third parties without user consent. Last September, the Swiss Federal Supreme Court [ruled](#) that IP addresses are personal data subject to the country's data protection law. According to [Linklaters](#), courts in Sweden, Spain and Austria have

reached similar conclusions.

Moves are afoot to similarly redefine device and location data. A researcher in New Zealand last month [discovered](#) that gaming company OpenFeint had successfully used smartphone user IDs and location data obtained during application installations and connected them with Facebook user profiles. In April, two researchers published a report claiming Apple's iPhone inappropriately collected and stored user-location data. The rapidity with which the U.S. Senate convened hearings about how Apple and Google manage user location data has put device makers, application developers and marketers on notice that they must take extra precautions when collecting or using this type of data.

At the same time, a lawsuit filed last month in U.S. District Court in Puerto Rico claimed that Apple, Pandora Media, and The Weather Channel were inappropriately disclosing personal data--unique device identifiers (UDIDs) and the location of those devices--to third-party ad networks. The ease of connecting a device with a named person prompted the EU's Article 29 Working Party in May to release an [opinion](#) that defines devices' location-based data as personal data subject to the EU Data Protection Directive.

"Location data is certainly, in many instances, private data, and there then follows the obligations to inform users, and the opportunity to opt in or opt out," said European Data Protection Supervisor Peter Hustinx.

Why are these redefinitions important? The vast numbers of Internet and software companies that collect and share clickstream data and device data as if it were aggregated, non-personal data may now be faced with obtaining Web visitor and user consent for these practices. Performing what used to be routine marketing analytics may become exceedingly difficult if higher forms of consent such as explicit permission emerge as the norm.

### **From personal data to sensitive PII**

Just as more non-personal data is becoming personal data, so too is more personal data becoming sensitive personal data subject to heightened security requirements. Two important developments occurred in April.

On April 1, Dallas-based Epsilon notified clients that it had suffered an unauthorized intrusion of its massive e-mail database. Although no information normally viewed as sensitive--such as credit card numbers, Social Security numbers or personal health information--was compromised, the incident highlighted the risk of spear phishing. Spear phishers use e-mail addresses from the same organization to first discover other information about those individuals and then to target them with fraudulent e-mails. To guard against this risk, companies are re-evaluating whether e-mail addresses should be upgraded to sensitive personal data.

On April 11, India released its long-awaited [Information Technology \(Reasonable security practices and procedures and sensitive personal data or information\) Rules 2011](#). These new rules define sensitive personal information somewhat differently than either the EU or United States to include passwords; personal financial information; physical, physiological and mental-health conditions; sexual orientation; medical records and history, and biometric information.

## **Outlook**

What are the implications of these changes?

A larger privacy footprint means greater demand for privacy professionals. More types of data requiring more security measures and use controls means there is more to do for in-house privacy staff and the attorneys and consultants who support them.

These changes also mean there will be more occasions for the privacy and marketing departments to work together. Up until this point, privacy staff might have been most concerned with high-risk personal data such as credit card information, personal health information and government IDs. But many of the data types that are getting upgraded are those used by marketing departments, who will now need more assistance to keep their projects on track.

Creque believes that organizations that adopt a Privacy by Design methodology will be more successful at navigating these data-classification changes and avoiding inadvertent uses and disclosures of personal data.

Organizationally, we also might be starting to see the disappearance of separate network zones and policies for the most sensitive personal data. If the trend continues toward all personal data receiving a high-risk classification, this rising common denominator may become the driving force converging global privacy regulations.

*Jay Cline is president of [Minnesota Privacy Consultants](#), the winner of the 2010 Privacy Innovation Award for Small Organizations.*